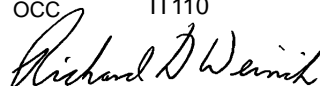


Management Instruction

Date	2/14/95
Effective	Immediately
Number	AS-850-95-2
Obsoletes	AS-850-91-1
OCC	IT110



Richard D. Weirich
Vice President
Information Systems

Request for Logon ID

This instruction explains how to acquire a computer logon ID and how to obtain, modify, or delete access to Postal Service computer systems using Form 1357, *Request for Computer Access*.

SCOPE

This instruction supersedes all prior directives pertaining to the completion and processing of Form 1357 and applies to all applicants requesting access to Postal Service computers.

DESCRIPTION

Form 1357 is the primary form used to obtain access to Postal Service computer systems, mainframe computer, minicomputer, and LAN-based applications. The form is used to establish new user IDs, add privileges to existing user IDs, and delete existing user IDs. It provides a means by which information systems personnel manage Postal Service system resources in accordance with the requirements specified by each system's executive sponsor.

Form 1357 is not used by the Inspection Service for requesting access to the Inspection Service information systems applications; internally developed forms are used instead. For information on the procedures for use of these internally developed forms, contact the postal inspector in charge.

NAMING STANDARDS

Logon ID naming standards are governed by the host system and software constraints. Standards fall into two general categories:

1. Mainframe.
2. Mini, micro, and/or LAN.

DEFINITIONS

Computer Logon ID – an identification code (a group of numbers, letters, and/or symbols) assigned to a computer user, programmer, operator, proxies, and computer-to-computer linkage. Used with a password, it allows the user, programmer, or operator to gain access to a computer system.

Logon ID Coordinator – the person responsible for processing logon ID requests at a site; may be the local systems administrator or IS manager.

Password – a unique string of characters that a computer user must provide (in conjunction with a logon ID) to meet security requirements before gaining access to computer system resources or data.

Nonpostal User – a United States citizen neither employed nor under contract with the Postal Service who has access to a postal computer.

Foreign User – a noncitizen of the United States who may or may not reside in the United States and who may be neither employed nor under contract with the Postal Service, but under special circumstances may be allowed access to postal computer systems.

REFERENCES

Administrative Support Manual (ASM)
HBK AS-802, *ADP Operating Standards*
HBK AS-805, *Information Systems Security*
HBK AS-818, *Local Area Network and
Personal Computer Security*

Mainframe Standards

Mainframe logon ID naming standards apply to computer systems that use the Access Control Facility (ACF-2) security system. Positions 3 and 4 of a mainframe logon ID may contain alphabetic characters identifying a minicomputer if the logon ID is used for computer-to-computer linkage. The minimum length is six characters. Positions 1 through 4 may also be used as identification codes at a local facility to describe the unit where the user is assigned.

Mini, Micro, and LAN Standards

Mini, micro, and LAN logon ID standards facilitate identification for user-to-user communication. Generally, the format of the logon ID is based on the user's last name, first initial, and/or middle initial. The minimum length is eight positions. The first six positions must consist of the first six letters of the user's last name. If the user's last name is shorter than six letters, the remaining positions up to position six will be filled with unique consecutive numeric digits starting with 01. Position seven will consist of the user's first initial. Position eight will consist of the user's middle initial. If the user does not have a middle name or initial, this position will be filled with unique consecutive numeric digits starting with 1. This standard is in force throughout the Postal Service unless technically prohibited by the operating system.

Exceptions

Exceptions to the above standards must be requested in writing stating the reason for the exception. Send the request to the manager of Information Systems Security at Headquarters. Logon IDs that do not conform to these standards but were in existence before issuance of these standards are not required to change.

ASSIGNMENT

A user is assigned a computer logon ID for his or her specific use in conducting postal business. To maintain individual accountability, computer logon IDs are assigned for individual use only and are not to be shared. However, computer logon IDs may be assigned for other purposes such as training, hardware maintenance, and special uses.

USER RESPONSIBILITIES

Users must comply with Postal Service computer security policies and procedures. All users of Postal Service computers (including career, casual, and temporary employees, contractors, nonpostal, and foreign users) are responsible for all uses of their assigned computer logon IDs. Logon IDs shall only be used for authorized Postal Service activities. Users will protect and conceal passwords at all times.

RESTRICTIONS

- To establish individual accountability, all logon IDs will be owned by an individual.
- The system or security manager will suspend a user logon ID that is inactive for a period of 180 days and will delete it if it remains inactive for a period of one year. Deletion of a logon ID in this case does not require completion of Form 1357.
- A logon ID controlled by ACF-2 software at Computer Operations Service Center (COSC) mainframes will be suspended after being inactive for a period of 90 days.
- Use of logon IDs may be restricted to specific locations or times. Logon IDs are subject to the rule of least privilege, i.e., only the minimum privilege a user requires to perform his or her duties will be granted.

PASSWORDS

Passwords must be a minimum of six characters. A password must not be the identical character string as the logon ID, e.g., if the logon ID is H813234, the password must not be H813234. A password must be a combination of characters that is not identifiable as a word for a place, thing, or name of a person or place, e.g., SHJMX, LLREQ2, or PTTGKW, but not ROBERT, DENVER, or KITTEN.

PRIVACY ACT CONSIDERATIONS

Computer logon ID records are covered by the Privacy Act. These records are maintained by the Postal Service in compliance with ASM Appendix, Privacy Act System of Records, USPS 150.030. They must be handled and disclosed only in accordance with the Privacy Act and the implementing instructions contained in the ASM. Those instructions give requirements for the collection, use, and disclosure of Privacy Act-protected information and the criminal penalties that may be assessed for failure to comply with the Act's provisions.

RECORDKEEPING

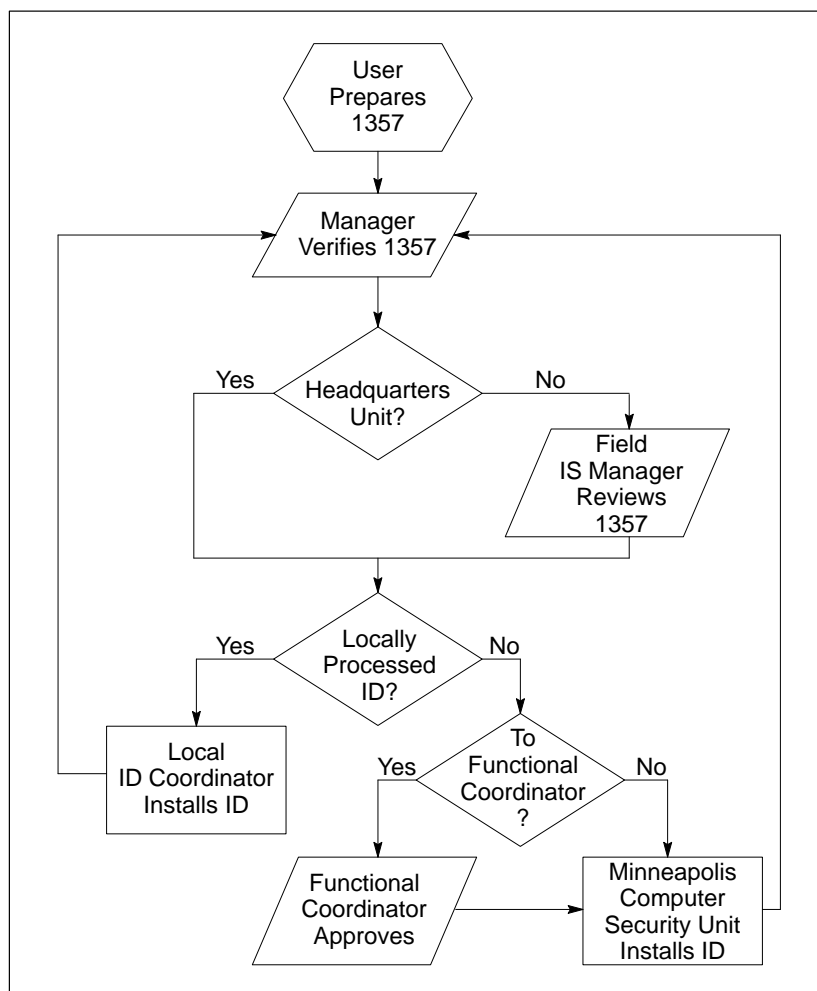
Records should be maintained as follows:

1. Completed Forms 1357 are kept at the site where the logon ID has been installed.
2. The original and copies of Forms 1357 must be kept in a secure file.
3. Forms for deleted and suspended logon IDs must be kept for two years from the date of deletion or suspension.

4. Original Forms 1357 with original signatures for logon IDs used for remote system management or remote application support must be filed at the issuing office.

PROCESS

Specific individuals are required to perform specific functions in the process of requesting logon IDs. The process followed depends upon whether the logon ID requested is for access to a mainframe or a local system (see Exhibit 1).



Logon ID Request Process

Exhibit 1

Requesting Access to Mainframe Systems

The process for requesting access to a mainframe computer system is as follows:

1. The user completes a Form 1357 and forwards it to his or her manager.
2. The manager verifies the information, signs the form, and forwards it to the field IS manager. If the user is at Headquarters, Form 1357 is sent to the functional coordinator (step 3 is skipped).
3. The field IS manager reviews the form for accuracy and proper signatures and forwards it to either the functional coordinator or directly to the Minneapolis Computer Operations Service Center (COSC) Security. (If unsure where to send the form, contact the Minneapolis COSC Security at (612) 725-1010.)
4. If applicable, the functional coordinator approves the request and forwards it to the Minneapolis COSC Security.
5. The Minneapolis COSC Security installs the logon ID and notifies the user of the access granted.

Requesting Access to Local Systems

The process for requesting access to a local computer system is as follows:

1. The user completes a Form 1357 and forwards it to his or her manager.
2. The manager verifies the information, signs the form, and forwards it to the field IS manager. If the user is at Headquarters, Form 1357 is sent to the local logon ID coordinator (step 3 is skipped).
3. The field IS manager reviews the form for accuracy and proper signatures and forwards it to a local logon ID coordinator.
4. The local logon ID coordinator installs the logon ID and notifies the user and the user's manager of the access granted.

Access to Sensitive Systems

If access is required to sensitive systems or applications, a user must complete other forms in addition to PS Form 1357. These can include Form 2013, *Sensitive Security Clearance Processing Request*; Form 2015, *Determination of Need for a Sensitive Clearance*; Form 2066, *Updated Personnel Security Questionnaire*; Form 2181, *Authorization and Release*; Standard Form 85P, *Questionnaire for Public Trust Positions*; and FD Form 258, *Fingerprint Chart*.

Modifying Access

A user with a valid logon ID will use Form 1357 to request access to additional computer data files or systems. The user's logon ID must be valid at the facility where the additional access is requested. Other access approvals from the functional coordinator or executive sponsor may be required before the additional access is assigned. For local in-house modification of logon IDs, electronic mail messages may be used to submit the request to the local security administrator.

Deleting Access

A user who no longer has a need for computer access must have his or her logon ID deleted from the system. The user's manager must request deletion of the logon ID using Form 1357. User logon IDs must be deleted in cases of termination, removal, reassignment, or contract expiration.

Contract, Nonpostal, and Foreign Users

Contract, nonpostal, and foreign users must comply with additional requirements before being granted access to Postal Service computers.

Contract Employees

A contract employee requesting access to postal service computers must be properly screened by the Inspection Service. A contract employee must have a sensitive clearance to have access to sensitive material. The screening and clearance procedure is described in ASM 272.3. A contractor cannot have unrestricted access to postal computers (including stand-alone PCs) until an interim or final screening has been completed by the Inspection Service. A contractor's logon ID can only be activated with an active audit or trace option until the results of the screening or clearance have been obtained. The contracting officer's representative (COR) is responsible for ensuring that a contract employee is screened or cleared by submitting the Form 1357 and the associated screening and/or clearance forms to the Inspection Service.

Adverse screening notification will result in the denial by the Inspection Service of computer access. In this situation, the Inspection Service will notify the COR and the logon ID coordinator. The contractor's logon ID will be suspended because of an adverse screening and access to Postal Service computers will be denied.

Contract employees with access to Postal Service computer resources must have that access terminated in the event of contract nonrenewal or other negative actions (suspension, dismissal, etc.). The COR will notify the logon ID coordinator of negative actions. The contract employee will have any access to postal service computer resources suspended.

Nonpostal and Foreign Personnel

A nonpostal or foreign user must submit a fully completed and signed Form 1357 to the sponsoring postal manager. Prior to approving the request, the sponsoring manager must acquire all necessary access approvals. Managers have the same responsibilities for foreign and nonpostal users as for Postal Service users. However, extra scrutiny and control is required, especially in:

1. Verifying that Form 1357 is completed correctly and signed.
2. Apprising the nonpostal or foreign users of the laws and regulations that apply to the user of a Postal Service logon ID.
3. Approving only the minimum access needed.

4. Deleting unneeded logon IDs promptly.

Faxed Copies

In emergency situations, copies of Form 1357 may be sent by fax in lieu of the original form. However, the form must be signed by both the user and his or her manager before it is faxed. The original must be sent to the logon ID coordinator within 10 working days of the receipt of the faxed copy.

Waivers and Exceptions

Waivers and exceptions may be granted by Information Systems Security in coordination with the Inspection Service.

LOGON ID MISUSE

All logon IDs must be protected from misuse. The use of a Postal Service computer for nonpostal business, games, security violations, unauthorized accesses, etc., is considered misuse or may present the appearance of misuse unless specifically authorized by the user's manager. Unauthorized use may result in disciplinary action and or prosecution. Any detected misuse of a postal computer or information system may be reported to the Inspection Service.

APPLICATION INFORMATION

The Minneapolis COSC Security maintains information on mainframe applications and a list of computer resources and access privileges under its authority. This organization will provide information, such as inventory of computer systems and applications, to users when requested. See phone number below.

ADDITIONAL INFORMATION

Contact the following organizations for further information concerning:

- The procedures described in this instruction.
- Up-to-date versions of any listings.
- Copies of forms or supplemental listings.

MINNEAPOLIS COMPUTER OPERATIONS	
SERVICE CENTER SECURITY	(612) 725-1010
INFORMATION SYSTEMS SECURITY	(202) 268-2741

For further information concerning the nature of individual applications or the correct specification of access privileges for a particular need, contact the application's designated point-of-contact in the list of current Postal Service applications. This list can be obtained from the Minneapolis COSC Security.